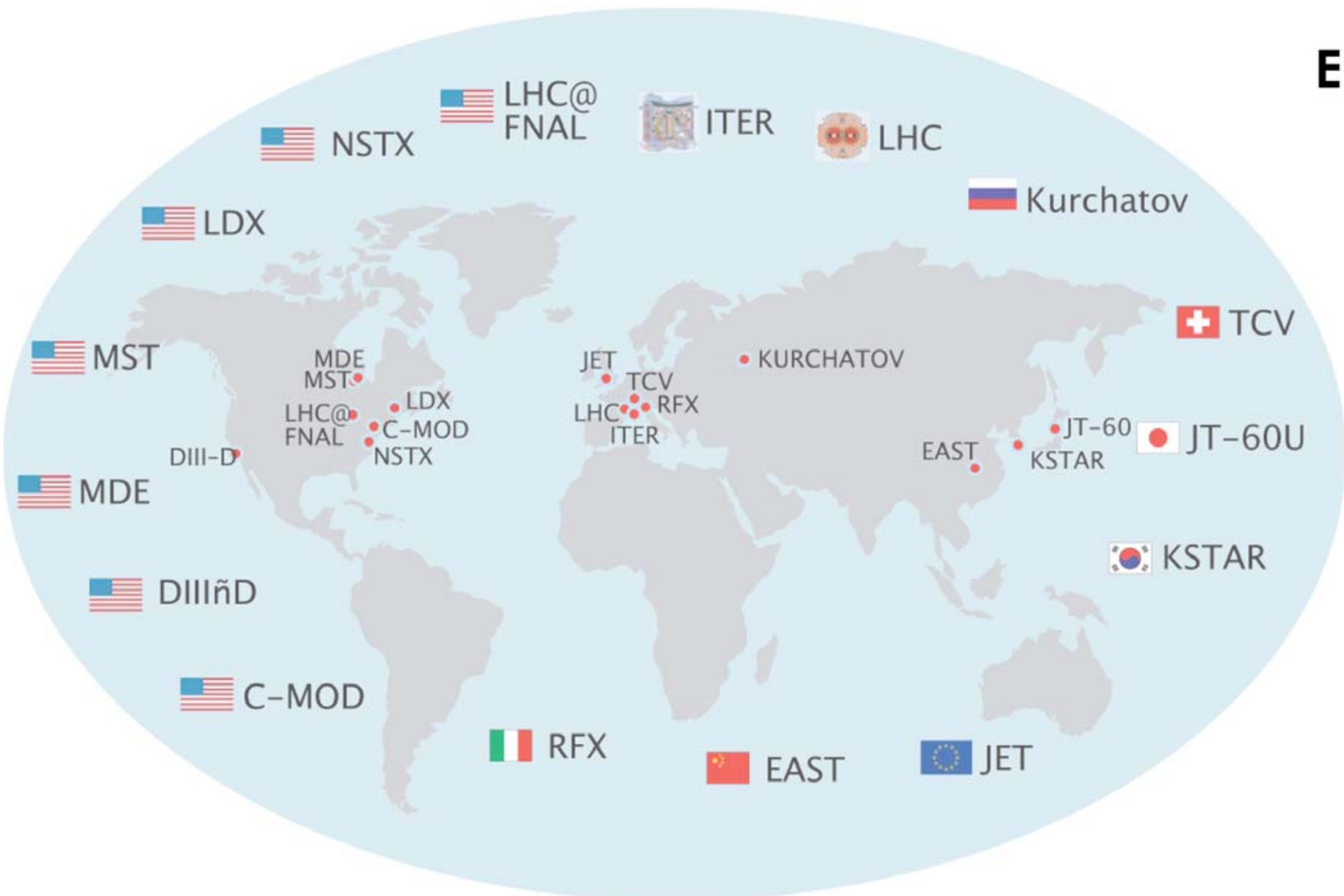
Thoughts on Joint Effort: OFES, OHEP, and OASCR



By

E. Gottschalk (FNAL)

D. Schissel (GA)

Presented at
DOE Headquarters

Germantown, MD

November 7, 2006

The Challenge: International, Remote Participation

- **Scientists will want to participate in "live" experiments from their home institutions, which are dispersed around the world**
  - View and analyze data
  - Manage instrumentation
  - Lead experimental sessions
  - Participate in remote shift activities

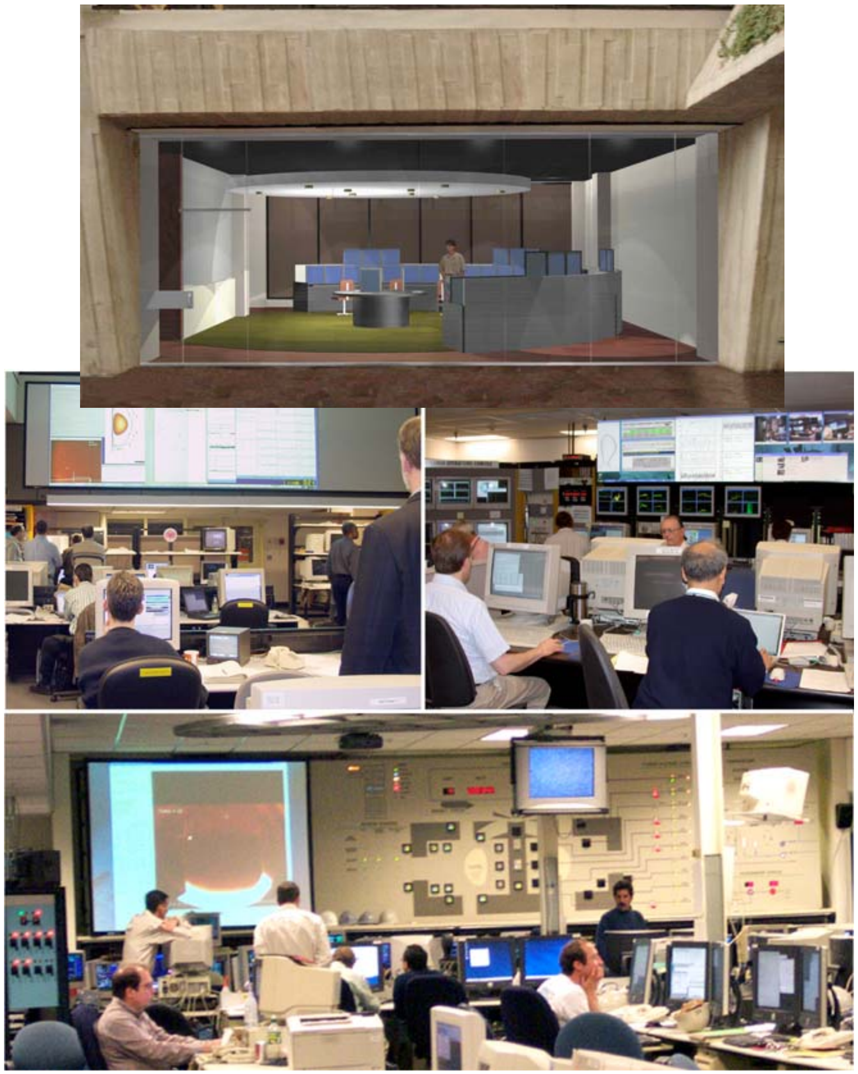
- **The requirements for remote participation are applicable at all times: before, during, and after an experiment**

- **Collaborations span many administrative network/security domains**
  - Resources managed by multiple groups, since local control is essential
  - Problem resolution spans multiple domains

- **Cyber security must be maintained, and security of experimental facilities must be inviolable.**

- **Safeguards need to be in place, so that actions do not jeopardize or interfere with operations.**

Both Remote and Distributed Operations have Challenges



- **Informal interactions and discussions in the control room are a crucial part of the research**

- **We must extend this into remote and distributed operations, and make it easier for people to communicate**

- **<u>Fully</u> involving remote participants in operations is also challenging**

- **Working as a distributed team goes beyond day-to-day operations**

The Requirements for HEP and FES are Similar

- **There is <u>substantial</u> overlap between HEP and FES requirements**
  - Support remote operations of experimental facilities, distributed code development, computing & visualization, operations planning
- **For FES the emphasis is on experimental and simulation data, while for HEP it is the mission-critical controls data that is important for operations**
  - Data must be securely available worldwide in near-real-time
- **Sharable applications and displays are needed for both HEP and FES**
  - Distributed science requires interactive scientific discussions
- **Improvements in interpersonal and group communication need to be integrated with data services**
  - This is not a present goal for the commercial world
- **We need prototype control rooms for design efforts for ITER and the ILC**

The overlap between HEP and FES requirements justifies joint research.

Work Scope Divided into two Main Areas

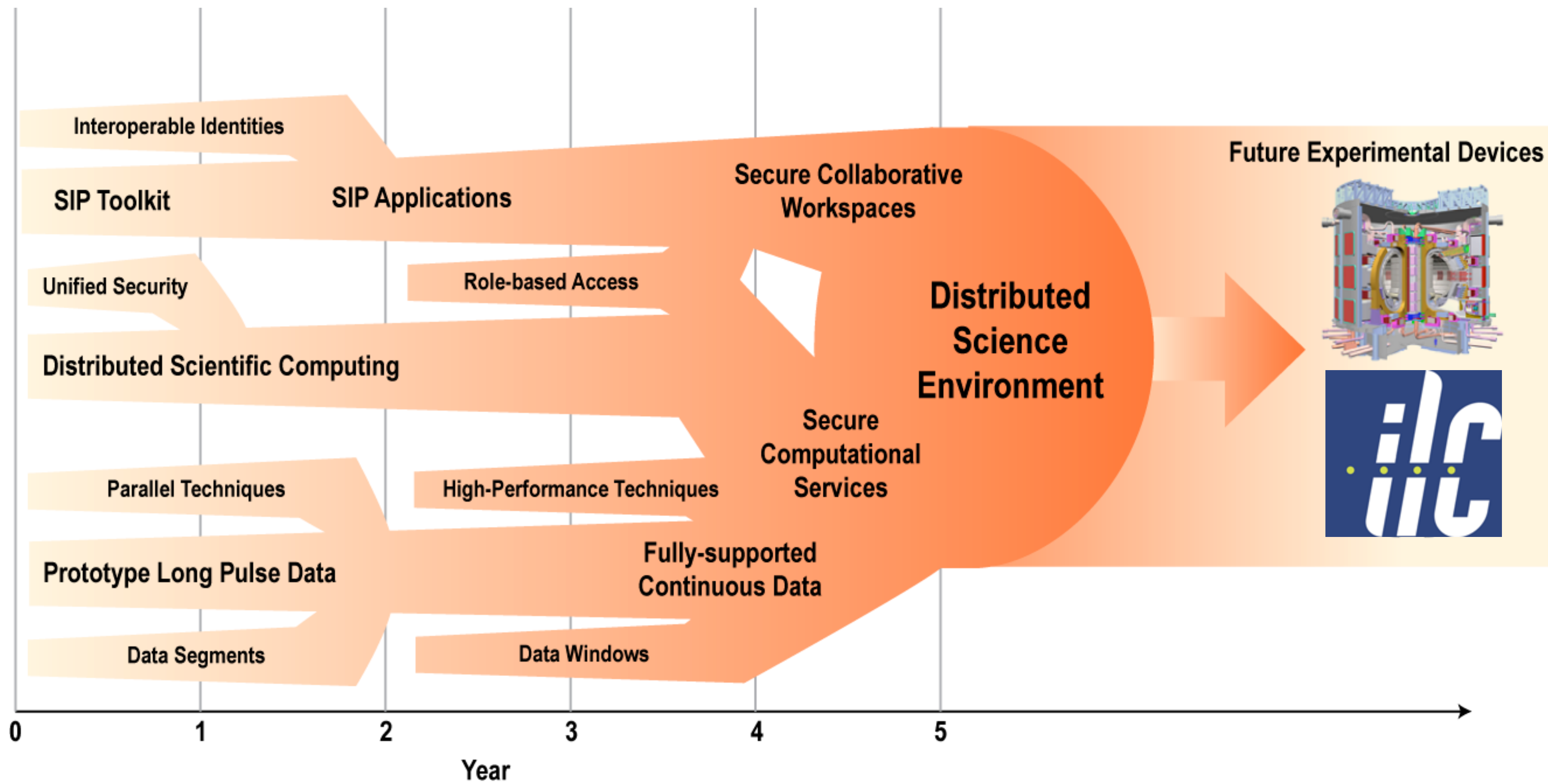
1. **"Collaborative Work Spaces" includes**
   - Extensible ad hoc & structured communications tools, which are
   - Standards-based, modular, role-aware, presence-aware, & web-friendly
   - Enhanced user agents: e.g. Access Grid, VRVS/EVO, VOIP phone
   - Shared displays and applications
   - Electronic Logbook

2. **"Secure Data Services" (near-real-time) includes**
   - Continuous acquisition and availability: e.g. long-pulse MDSplus
   - Sequenced Data Acquisition (SDA)
   - International Grid interoperability:Russia (RDIG), Europe (EGEE), OSG

Security enhancements apply to both areas
- Enhanced, easier-to-use security: e.g. UCAM, IDDB
- Heterogeneous, integrated and role-aware security

Original Proposal Request: OFES – $1M, OHEP – $0.5M, OASCR – $0.9M

The Long Term Vision Integrates Capabilities to Enable Distributed Science for HEP and FES



Remote Participation Requires Ad Hoc Communications

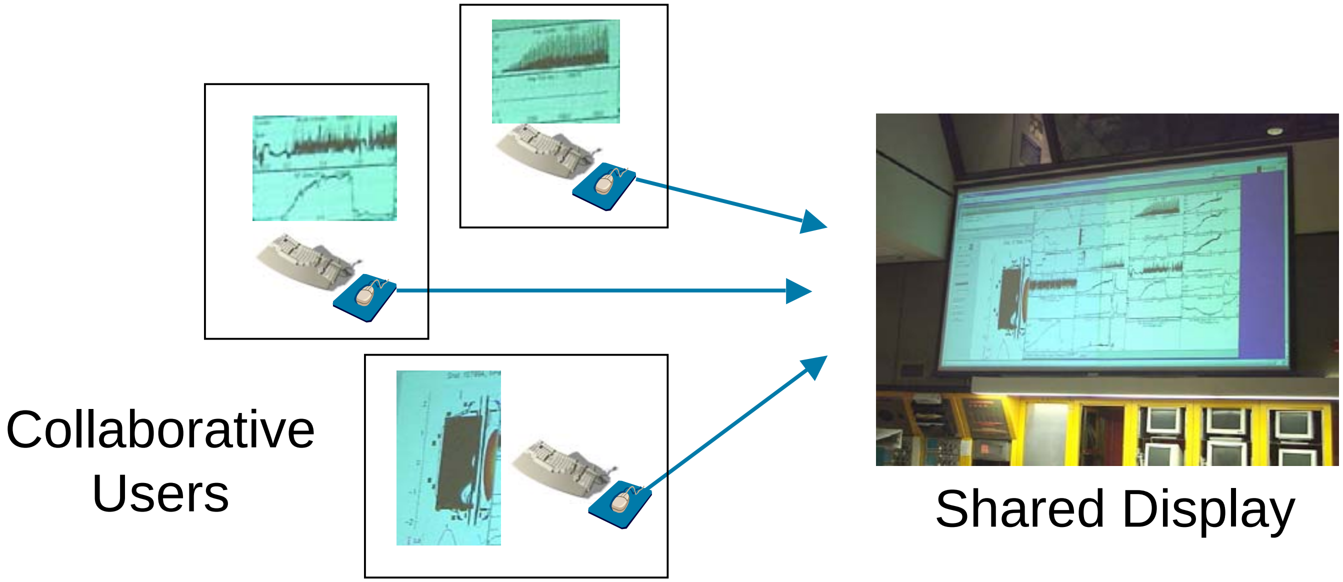
- **Goal is to exploit convergence of telecom and internet technologies (e.g. SIP)**
- **Deploy integrated communications**
  - Voice
  - Video
  - Messaging
  - E-mail
  - Data

- **Implement advanced directory services**
  - Identification, location, scheduling
  - “Presence”
  - Support for “roles”
- **Integrate SIP into user agents**
  - For example, Access Grid & VRVS/EVO

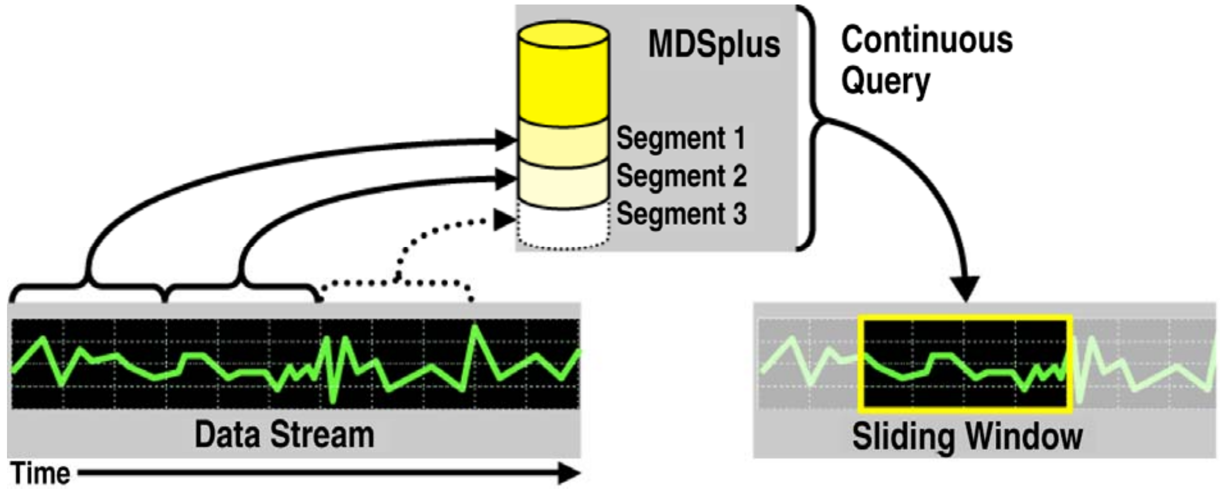
Remote Participation Requires Shared Displays and Applications

- **There is a need for distributed, shared display walls for**
  - Remote collaborative visualization in control rooms and on desktops
  - A distributed shared display protocol is required
  - Multi-party updates require appropriate security

- **There is a need for network bandwidth optimization to**
  - Overcome network latency and bandwidth limitations
  - Combine intelligent caching with compression



Require Secure Near-Real-Time Data Services



- **Requirements call for concurrent writing, reading, analysis, visualization of data**

- **FES data will span a range >10^9 in significant time scales**
  - Long-pulse or continuous MDSplus

- **Sequenced Data Acquisition (SDA)**
  - To define specific "events" or "stages" for data analysis

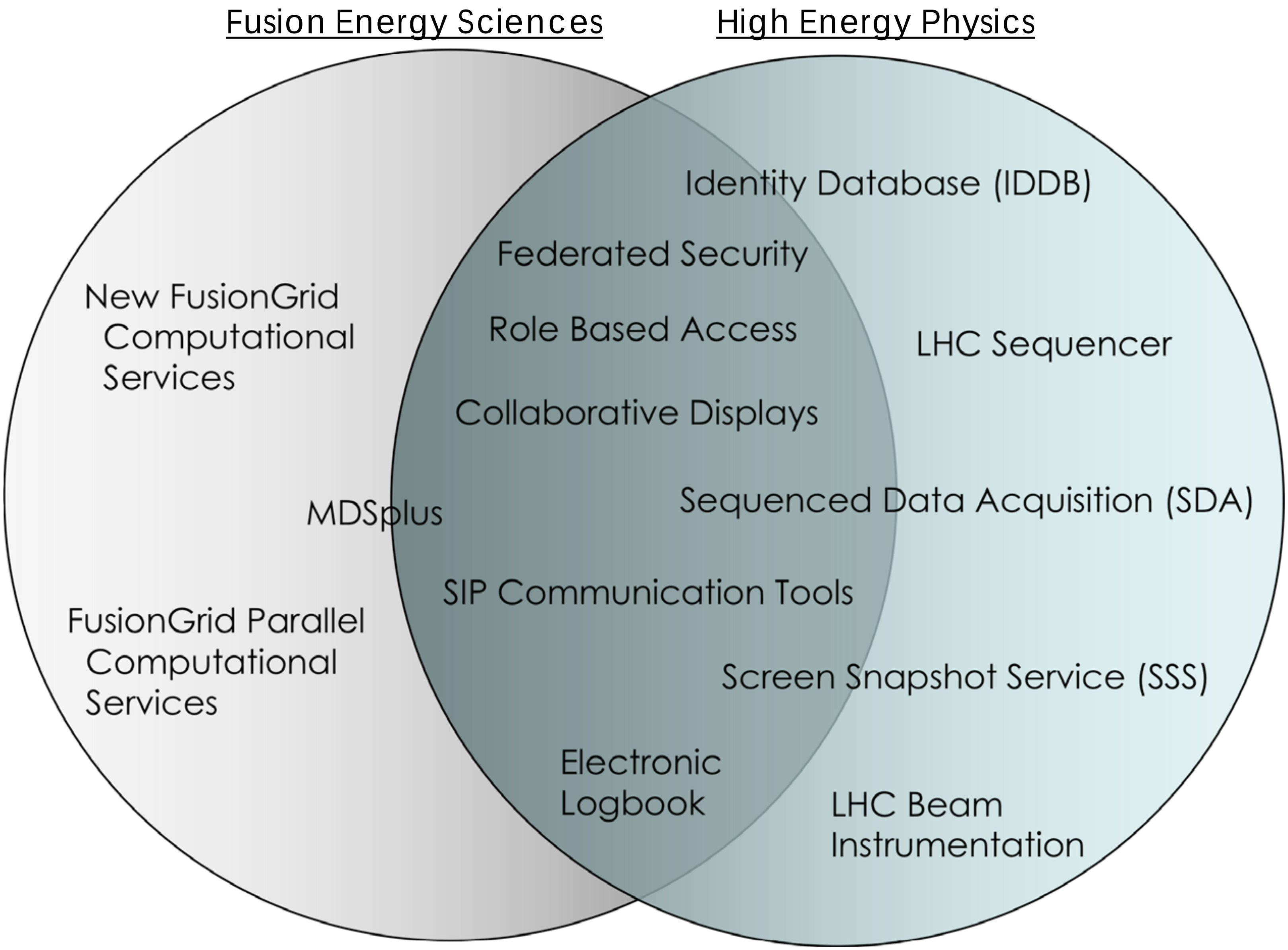
- **Data services will require efficient tools**
  - To browse very long records

Federated Security

- **Intrinsic conflict between ease-of-use and strong security**
  - Requires lowering user friction
- **UCAM: User, Credential, and Authorization Manager (also IDDB)**
  - Appropriate for international grids with heterogeneous authentication
  - For example: One Time Password (OTP) and dynamic firewalls
- **Federated Web Portals implemented with PubCookie**
  - Single sign-on for a Grid certificate based web system

- **We require a more versatile authorization policy**
  - Dynamic role-based authorization
- **Grid interoperability**
  - e.g. Russian Data Intensive Grid (RDIG), European Data Grid (EGEE), and Open Science Grid (OSG)

Substantial Overlap Between FES and HEP Needs



Substantial Support Domestically and Internationally

Support from FES Experimental Projects

Sir Llewellyn Smith: Head Euratom/UKAEA Fusion Association
Dr. Marmar: Head, Alcator C-Mod
Dr. Stambaugh: Director, DIII-D
Dr. Ono: Head, NSTX
Dr. Fonk: Director, U.S. Burning Plasma Organization
Dr. Mauel: PI, LDX
Dr. Sarff: Co-PI, MST
Dr. Forest: Co-PI, MDE
Dr. Smirnov: Director, Kurchatov Institute, Russia
Drs. Ongena, Buttery, Voistekhovitch: Task Force Leaders, JET Project, UK
Dr. Li, Director: EAST, China
Dr. Ninomiya: Director, Division of Plasma Research, JAEA, Japan
Dr. Kwon: Director, KSTAR, South Korea
Drs. Duval, Llobet: Scientists, TVC and CRPP Fusion Facilities, Switzerland
Dr. Manduchi: Lead, Control and Data Systems, RFX Fusion Facility, Italy

Substantial Support Domestically and Internationally

Support from FES Simulation Projects

Dr. Chang: Lead-PI
SciDAC FSP Center for Plasma Edge Simulation Project

Dr. Jardin: Lead-PI
SciDAC CEMM Project

Dr. Batchelor: Lead-PI
SciDAC SWIM Project

Dr. Bonoli: Lead-PI
SciDAC Center for Wave-Plasma Interactions Project

Dr. Dorland: Lead-PI
GS2 Software Project

Support from High-Energy Physics Projects

Dr. Schmickler, Head,
CERN AB-CO Controls Group

Dr. Bauerdick, Head,
U.S. CMS Software & Computing

Dr. Peggs, Leader,
U.S. LHC Accelerator Program

Dr. Green, Manager,
U.S. CMS Research

Dr. Kephart, Director,
Fermilab ILC HEP Program

OASCR Involvement is Critical to Success

- **Collaborative technologies are critical to many SC programs**
- **Development effort needs expertise that is available outside of the science programs**
- **Collaboration with Computer Science community has certainly been important to the SciDAC program**
- **Note - Needs of science programs go beyond petascale computing**
- **OASCR expertise can assist with many aspects of the proposed work:**
  - SIP standards-based components w/ presence and role-based features
  - Security: Federated Web portals, UCAM, Grid-site security interaction
  - Distributed shared displays and network bandwidth optimization
  - Access Grid: implementing SIP and addressing interoperability issues

Concluding Comments

- **Both the FES and HEP programs are working on collaborative tools**
  - FES: emphasis on domestic program, international efforts, and ITER
  - HEP: LHC and the ILC

- **There is a clear vision & work scope for the "Collaborative Control Room"**
  - Real-time support for experiments is critical
  - The concept includes most, if not all, FES and HEP collaborative needs
  - Clear software enhancements required for success

- **We envision a path to success that benefits FES and HEP and leverages OASCR**

- **What are the next steps to keep this going?**

Additional Slides

Role Based Access (RBA)

An approach to restrict system access to authorized users.

What is a ROLE**?**

- **A role is a job function within an organization.**
- **Examples: LHC Operator, SPS Operator, RF Expert, PC Expert, Developer, …**
- **A role is a set of access permissions for a device class/property group**
- **Roles are defined by the security policy**
- **A user may assume several roles**

What is being ACCESSED**?**

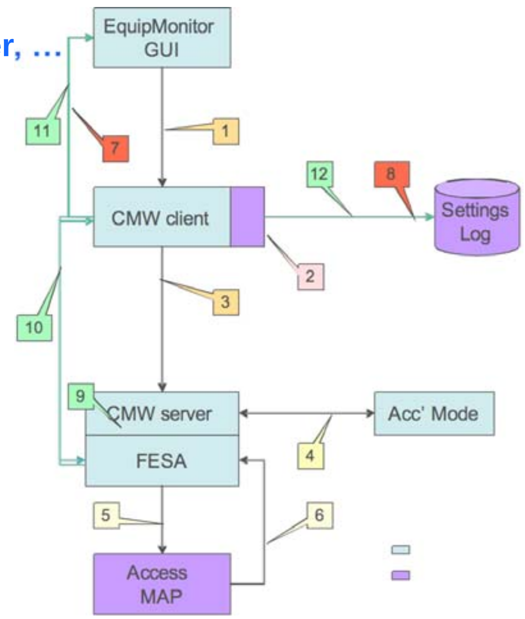
- **Physical devices (power converters, collimators, quadrupoles, etc.)**
- **Logical devices (emittance, state variable)**

What type of ACCESS**?**

- **Read: the value of a device once**
- **Monitor: the device continuously**
- **Write/set: the value of a device**

Requirements have been written

- **Authentication**
- **Authorization**



Status: Design document in progress

The software infrastructure for RBA is <u>crucial</u> for remote operations. Permissions can be setup to allow experts outside the control room to <u>read or monitor a device safely</u>.

This is a Fermilab/CERN collaboration working on RBA for the LHC control system.

LHC Sequencer

Automates the very complex sequence of operations required to operate the LHC.

Typical commands

- Set, get, check devices
- Wait for conditions
- Execute more complex operations
- Start regular programs
- Start plots
- Send data to shot log

Step through commands

- Stops on error
- Allow restart at failed command

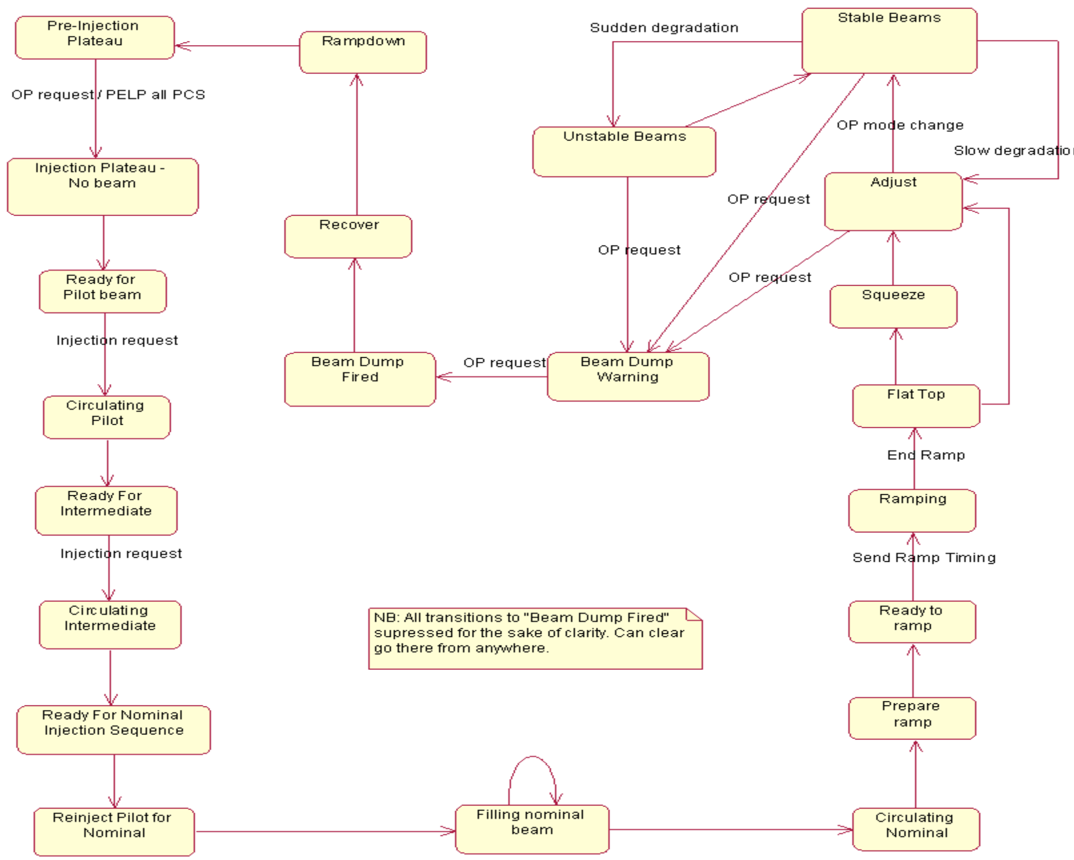
Sequencer is used for:

- Normal operations
- Studies or special cases

Working with CERN on requirements

- Explore existing implementations: FNAL, LEP, RHIC, NIF, HERA, SMI++
- http://cd-amr.fnal.gov/remop/Sequencer.htm

LHC State Diagram



This is a Fermilab/CERN collaboration working on the LHC Sequencer.

Sequenced Data Acquisition (SDA)

SDA is a software system for collecting, storing and analyzing data in terms of the stages of a complex process.

SDA 1

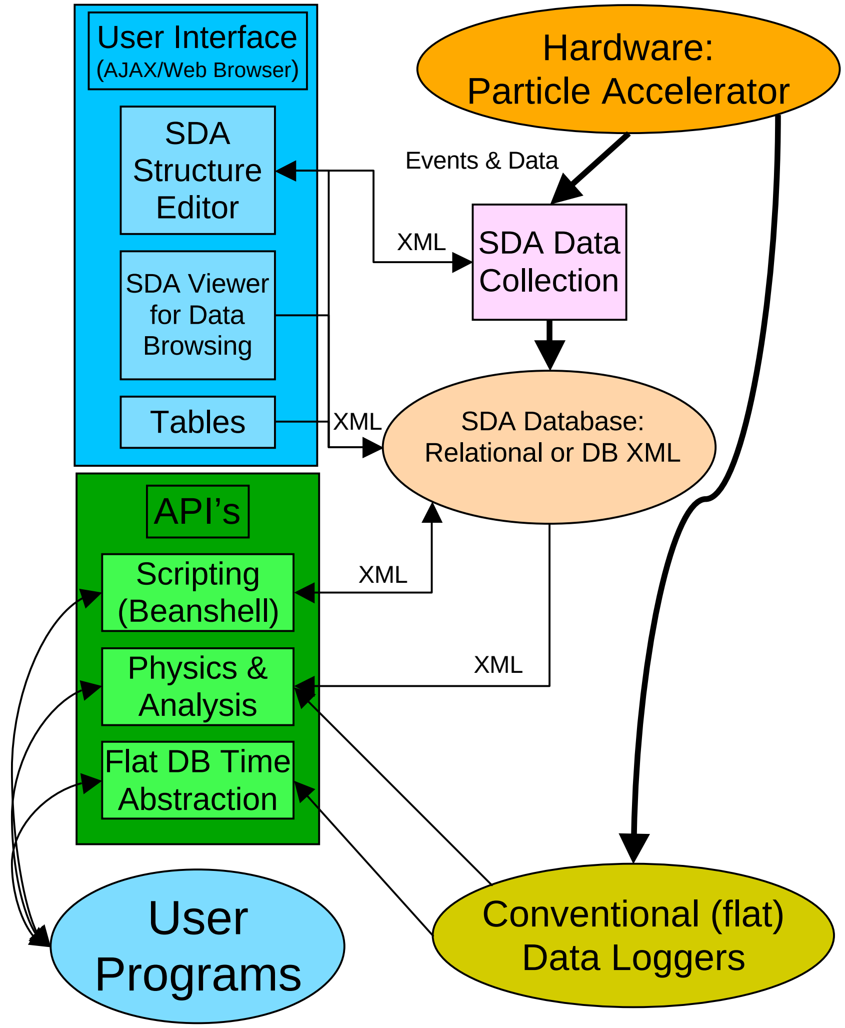
- 1st version of SDA developed for FNAL Run II
- Provides consistent and accurate data from the Fermilab accelerator complex
- Used by operators, physicists, engineers, DOE

SDA 2

- 2nd version of SDA being developed
- Improved SDA for FNAL
- Development is ~90% completed

SDA 2 for LHC

- Need to establish requirements for LHC with CERN
- “SDA Workshop” on Nov. 16 at CERN



This is a Fermilab/CERN collaboration.

Screen Snapshot Service (SSS)

An approach to provide a snapshot of a graphical interface to remote users.

What is a snapshot?

- An image copy of a graphical user interface at a particular instance in time.
- Examples: DAQ system buffer display, operator control program, …
- A view-only image, so there is no danger of accidental user input.
- Initially envisioned for application GUIs but could be expanded to desktops.

What is the role of the service?

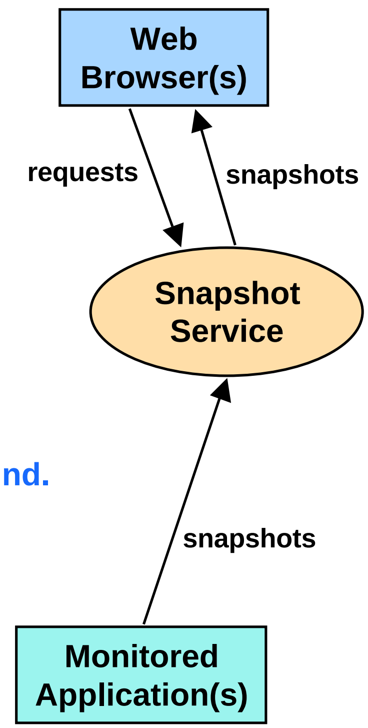
- Receives and tracks the snapshots from the monitored applications.
- Caches the snapshots for short periods of time.
- Serves the snapshots to requesting applications/users.
- Prevents access from unauthorized applications/users.
- Acts as a gateway to private network applications for public network users.

How will this work?

- Applications capture and send snapshots to the service provider in the background.
- Users would access snapshots using a web browser.

Status:

- The capturing of snapshots from Java applications has been demonstrated.
- The transfer of snapshots is being investigated.



SSS is being developed at Fermilab for CMS, and may be applicable to the LHC.

Identity Database (IDDB)

A lightweight user authentication framework.

Motivation

In order to enable access control in software applications, users need to be properly authenticated. This requires a security infrastructure that maintains user accounts, permissions, and has access to log files. A typical developer usually does not have enough time and expertise to implement and maintain a security infrastructure.

Identity Database

A solution that targets small- and medium-scale applications, both standalone and web-based, such as programs for data analysis, web portals, and electronic logbooks.

Features

- Includes database, application programming interface (API), and web-based user interface for management.
- A single IDDB instance can be shared by multiple programs/systems.
- A single user can be identified by several different types of credentials: username + password, Kerberos, X.509 certificates, IP address
- Access permissions are described by roles, and roles are assigned to users.
- Each application can have its own set of roles, which are managed independently.

IDDB is being developed at Fermilab for an electronic logbook for ILC.

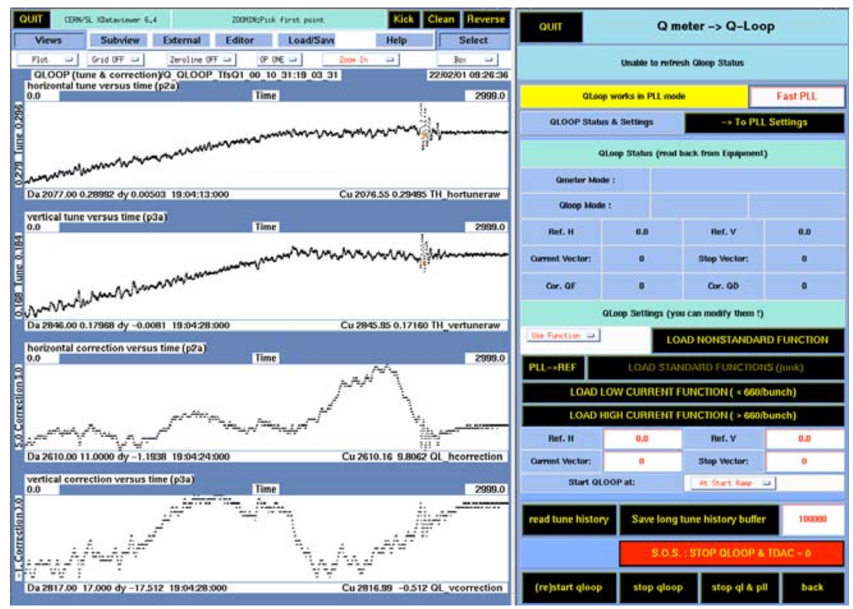
LHC Beam Instrumentation Software

Dedicated applications for LHC beam instrumentation still need to be written.

- Tune measurement (including coupling, chromaticity, etc.)
- Wire scanners, synchrotron radiation monitors, etc.

The LHC@FNAL Software (LAFS) team will begin by writing the high-level application software for the LHC tune measurement system by providing panels for device configuration/setup and measurement displays:

- FFT measurement
- Continuous FFT
- Tune PLL
- Chromaticity measurement
- Tune feedback
- Coupling feedback



This is a Fermilab/CERN collaboration working on LHC beam instrumentation software.